

Appl. No.: 09/645,376
Filed: August 24, 2000
Amdt. Dated June 6, 2008
Reply to Office Action of May 7, 2008

REMARKS

In the Office Action dated May 7, 2008, Claims 4, 7, and 14 are rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Pat. No. 5,870,474 to Wasilewski et al. (“Wasilewski”) in view of U.S. Pat. No. 6,480,831 to Cordery et al. (“Cordery”). Claims 1-3, 6, and 8-13 are allowed. Applicant appreciates Examiner’s thorough examination of the present application and allowance of Claims 1-3, 6, and 8-13. As explained below, Applicant respectfully submits that Claim 4 and by dependency Claims 7 and 14 are also patentably distinct from the cited references, viewed alone or in combination. As such, in light of the subsequent remarks, Applicants respectfully request reconsideration and allowance of all of the pending claims of the present application.

Independent Claim 4 and Dependent Claims 7 and 14 are Patentably Distinct from the Cited References

Independent Claim 4 is directed to a method for decrypting a message received over a broadcast network that includes: (i) receiving data comprising an encrypted message and a hashed key at a node in the broadcast network, (ii) parsing the data to derive the encrypted message and the hashed key, (iii) comparing the received hashed key with a plurality of keys that are prestored at the node and selecting a key having a hash that matches the received hashed key, (iv) decrypting the encrypted message with the matching key if a match was found, and (v) requesting a key from a network entity if no prestored key is found to have a hash that matches the received hashed key.

Independent Claim 4 is rejected under 35 U.S.C. § 103(a) as being obvious in view of Wasilewski and further in view of Cordery. The Office Action admits that Wasilewski does not teach or suggest requesting a key from a network entity if no prestored key is found to have a hash that matches the received hash key and instead relies on Cordery as teaching this recitation. Applicant respectfully submits, however, that Cordery also does not teach or suggest requesting a key from a network entity if no prestored key is found to have a hash that matches the received hash key.

In this regard, Cordery is directed to a method and apparatus for securely transmitting keys from a postage metering apparatus to a remote data center. Cordery accordingly teaches periodic changing of cryptography keys used by postage metering systems and verified by a verification authority, such as the post office by securely transferring newly generated public keys from a postage metering system to a verification authority (referred to as a “data center”). The method taught by Cordery includes the postage metering system transmitting a newly generated public key, additional data, and encrypted hash to the data center. *See, e.g.* Col. 4, lines 64-67 of Cordery. Cordery then teaches the data center verifying the authenticity of the received newly generated public key by decrypting the received encrypted hash using the previous public key. Cordery then teaches the data center creating its own hash based on the received new public key and various additional data and then comparing the hash value created by the data center to the received hash value. If the hash values do not match, the data center generates an error message to the postage metering center. If, however, the hash values match, the data center acknowledges acceptance of the received new public key. *See, e.g.* Col. 5, lines 1-38 of Cordery.

In contrast to Cordery, which teaches locally calculating a hash value based upon and in response to receiving a new public key and additional data and comparing the calculated hash value to a received hash value, independent Claim 4 recites requesting a key from a network entity if no prestored key is found to have a hash that matches said received hashed key. Thus, while Cordery teaches comparing a locally calculated hash value to a received hash value, Claim 4 recites looking for a prestored key having a hash that matches a received hashed key. Further, even ignoring the above-described differences in Cordery and Claim 4, Cordery does not teach or suggest requesting a key in the event compared values do not match, as Cordery at most teaches generating and sending an error message. Applicant therefore respectfully submits that Cordery does not teach or suggest requesting a key from a network entity if no prestored key is found to have a hash that matches the received hash key and thus none of the cited references, taken alone or in combination teach or suggest requesting a key from a network entity if no prestored key is found to have a hash that matches the received hash key. Therefore, the

Appl. No.: 09/645,376

Filed: August 24, 2000

Amdt. Dated June 6, 2008

Reply to Office Action of May 7, 2008

rejection is overcome and Applicant respectfully submits independent Claim 4 is in condition for allowance. Since dependent Claims 7 and 14 each include all of the recitations of independent Claim 4, Applicant further submits that dependent Claims 7 and 14 are patentably distinct over the cited references, taken alone or in combination, for at least the reasons discussed above.

Appl. No.: 09/645,376
Filed: August 24, 2000
Amdt. Dated June 6, 2008
Reply to Office Action of May 7, 2008

Conclusion

In view of the remarks presented above, it is respectfully submitted that the claims of the present application are in condition for allowance. It is respectfully requested that a Notice of Allowance be issued in due course. The Examiner is requested to contact Applicants' undersigned attorney to resolve any remaining issues in order to expedite examination of the present application.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,



Charles A. Leyes
Registration No. 36,898

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON June 6, 2008.

LEGAL02/30122888v1